METHOD AND APPARATUS FOR OBTAINING STATUS OF PUBLIC KEY CERTIFICATE UPDATES

Abstract of the Disclosure

A method and apparatus for public key certificate updates is accomplished when a user of a secured communications system provides, from time to time, a public key certificate update subscription update to a server. The public key certificate update subscription information identifies at least one subscriber subject (i.e., another end-user) that the user desires to obtain real time public key updates when they occur. In response to the subscription information, the server monitors public key certificates of the at least one subscriber subject. When a change occurs to the public key certificate of the at least one subscriber, the server provides an indication of the change to the requesting user. As such, while the user is on-line with the secured communications system, the server can provide the user with real-time updates of subscriber subjects' encryption public key certificates and/or signature public key certificates. In addition, or as an alternative, to providing the subscription information, the user may provide an indication of a local replica of the public key certificates that it has stored to the server. Upon receiving the replica, the server determines whether the user's replica is consistent with the system's most current public key certificates of the subscriber subjects. If the user's replica is consistent with the current public key certificate, the server provides no response to the user or provides a response indicating that the user's list is current. If, however, the user's replica is not consistent with the current public key certificate, the server provides an indication of the differences to the user. The indication allows the user to update its local lists to be consistent with the most current public key certificate list.